

FF

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-288973

(43)Date of publication of application : 28.11.1990

(51)Int.Cl. G06F 15/30
G06F 15/00
G06K 17/00
G07F 7/12

(21)Application number : 01-051554

(71)Applicant : RICOH CO LTD

(22)Date of filing : 03.03.1989

(72)Inventor : SHOJI HIROYUKI
FURUTA TERUYUKI

(30)Priority

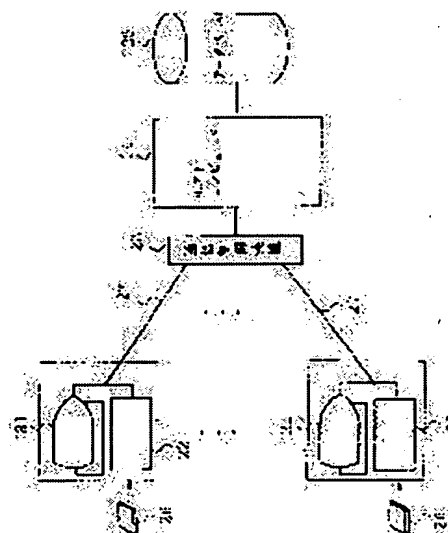
Priority number : 64 2312 Priority date : 09.01.1989 Priority country : JP

(54) SYSTEM FOR PROTECTING PRESUMPTION OF PASSWORD

(57)Abstract:

PURPOSE: To heighten the security of a system by displaying camouflage information and taste information set at every digit corresponding to an access key, and confirming a password by collating information selected and inputted from a display content by a customer with the taste information registered on a card.

CONSTITUTION: The output picture data of the camouflage information(Camouflage Information:CI) including the information of credit balance and transaction specification, etc., and individual taste information(Individual Taste Information:ITI) used in the definition of the password is registered on a data base 25. Also, a host computer 24 stores a program for the confirming processing of the password. And a owner confirming processing is performed by displaying the output picture data accumulated in the data base 25 on terminal equipment 21 according to the information read from the card 26 inserted by the customer and collating data selected and inputted from the terminal equipment 21 by the customer according to the above display with owner identification information set in advance, and furthermore, an automatic transaction is performed. In such a way, the security of the system can be heightened than ever.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑫ 公開特許公報(A)

平2-288973

⑤ Int. Cl.⁵

G 06 F 15/30
 15/00
 G 06 K 17/00
 G 07 F 7/12

識別記号

3 4 0
 3 3 0 F
 V

庁内整理番号

6798-5B
 7361-5B
 6711-5B

⑬ 公開 平成2年(1990)11月28日

8208-3E G 07 F 7/08

C

審査請求 未請求 請求項の数 2 (全17頁)

⑭ 発明の名称 暗証番号の推測防護方式

⑮ 特 願 平1-51554

⑯ 出 願 平1(1989)3月3日

優先権主張 ⑰ 平1(1989)1月9日 ⑱ 日本(JP) ⑲ 特願 平1-2312

⑳ 発 明 者 庄 司 浩 之 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 ㉑ 発 明 者 古 田 輝 幸 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 ㉒ 出 願 人 株 式 会 社 リ コ ー 東京都大田区中馬込1丁目3番6号
 ㉓ 代 理 人 弁 理 士 磯 村 雅 俊

明 細 書

1. 発明の名称

暗証番号の推測防護方式

2. 特許請求の範囲

(1) 本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、上記カードには、個人的な嗜好や特徴を含む情報を基にして各桁の番号を定義した暗証番号と、該暗証番号の各桁毎に設定された偽装情報へのアクセスキーとを含むデータを登録し、上記システムには、該アクセスキーに対応する該偽装情報を含むデータを格納して、顧客が挿入したカードにより該暗証番号の各桁の番号を照合して本人であることを確認する場合には、該アクセスキーに対応して各桁毎に設定した該偽装情報、および該嗜好情報を表示して、顧客が表示内容から選択・入力した情報と該カードに登録された該嗜好情報とを照合して、該暗証番号を確認することを特徴とする暗証番号の推測防護

方式。

(2) 本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、該システムには、ID番号、本人確認を行う際の照合コードの生成に用いるアルゴリズム、該照合コードの構成、および該アルゴリズムの演算要素として用いる乱数の桁数を含むデータを登録し、顧客が上記カードを用いて該システムへアクセスする場合には、該システムは該カードからID番号を読み取り、該乱数桁数に従って乱数を発生して表示するとともに、登録されたアルゴリズムに該乱数を代入して照合コードを生成し、該照合コードと、顧客が入力したコードとを比較照合して、本人確認を行うことを特徴とする暗証番号の推測防護方式。

3. 発明の詳細な説明

〔技術分野〕

本発明は、暗証番号を利用して本人確認を行う銀行システム等における暗証番号の推測防護方式に関し、特に、システムのセキュリティを高める

ことが可能な暗証番号の推測防護方式に関する。

〔従来技術〕

従来、銀行システム等では、各種サービスを行う際に顧客本人であることを確認するため、予め顧客毎に暗証番号を決め、その暗証番号を利用して本人確認を行っていた。また、暗証番号には数値4桁程度の組み合わせの固定コードが採用され、顧客は記憶し易い番号(例えば生年月日等)を設定していた。

この暗証番号は主に人間の記憶によって保護されているため、大幅に桁数を増やすことは難しい。このため、顧客が設定した暗証番号を、第3者が推測し、被害届が出されるまで繰返し不正使用されることがあった。

さらに、桁数の多いコードを採用したり、推測され難い数字を登録した場合でも、そのコードを記憶するためのメモ等が必要となり、メモを紛失すると本人でもアクセスできなくなる。

また、コンピュータサービスシステムでは、コンピュータ端末を使ってアクセスする場合等、不

正な利用者が思いついたコードによるアクセスを試行してパスワードを探り当てる恐れがあった。

なお、コンピュータ・システムのセキュリティについては、例えば“デー・ダブリュー・デービス、ダブリュー・エル・プライス著、セキュリティ フォー コンピュータ・ネットワーク、ジョン・ウィリー アンド サンズ、1984、(D.W. Davies, W.L. Price: Security for computer networks, John Wiley & Sons, 1984)”において論じられている。

〔発明が解決しようとする課題〕

上記従来技術では、暗証番号の桁数を増加したり、固定コード以外の照合コードを登録することによって、システムのセキュリティを高めることが難しかった。

本発明の目的は、このような問題点を改善し、システムのセキュリティを高めることが可能な暗証番号の推測防護方式を提供することにある。

〔課題を解決するための手段〕

上記目的を達成するため、本発明の暗証番号の

- 3 -

推測防護方式は、本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、上記カードには、個人的な嗜好や特徴を含む情報を基にして各桁の番号を定義した暗証番号、その暗証番号の各桁毎に設定された偽装情報へのアクセスキー等を登録し、上記システムの出力画面データファイルには、そのアクセスキーに対応する偽装情報を格納して、顧客が挿入したカードにより暗証番号の各桁の番号を照合して本人であることを確認する際、画面制御部の制御により、アクセスキーに対応して各桁毎に設定した偽装情報、および嗜好情報を表示して、顧客がその表示内容から選択・入力した情報とカードに登録された嗜好情報とを照合処理部で照合して、その暗証番号を確認することに特徴がある。

また、本発明の暗証番号の推測防護方式は、本人であることを確認するための情報を予め登録したカードを使用して、顧客にサービスを提供するシステムにおいて、そのシステムのアクセスコー

- 4 -

ド情報ファイルには、上記カードのID番号、本人確認を行う際の照合コードの生成に用いるアルゴリズム、その照合コードの構成、およびそのアルゴリズムの演算要素として用いる乱数の桁数を含むデータを登録し、顧客がカードを用いてシステムへアクセスする場合には、システムのアクセスコード情報読取部はそのカードからID番号を読み取り、乱数発生処理部は登録された桁数に従って乱数を発生して、その乱数を顧客に対して表示するとともに、アクセスキーコード作成処理部は登録されたアルゴリズムにその乱数を代入して照合コードを生成し、入力コード照合処理部によってその照合コードと、顧客が入力したコードとを比較照合して、本人確認を行うことに特徴がある。

〔作用〕

本発明においては、個人的な嗜好や特徴を含む情報を基にして暗証番号の各桁を定義し、本人確認を行う際は、その暗証番号の各桁毎に設定された偽装情報を表示して、選択・入力させるため、

顧客に負担を与えることなく、暗証番号の桁数を増加することができる。

また、本発明においては、本人確認に用いる照合コードとして、固定された数字列を用いず、その照合コードを生成するためのアルゴリズムを登録し、そのアルゴリズムの演算要素として、システムが発生させた乱数、あるいは年月日、時刻、曜日、任意の変数等を用いるため、本人以外の不正な使用者が照合コードを類推することは難しい。

これらの方法を採用することにより、システムのセキュリティをより高めることが可能である。

〔実施例〕

以下、本発明の一実施例を図面により説明する。

まず、本発明の第1の実施例について述べる。

第2図は、本発明の第1の実施例における自動取引システムの構成図である。

本実施例の自動取引システムは、銀行の各店舗毎に端末装置21およびカード読取装置22を備え、銀行の顧客は本人確認情報(暗証番号)を記憶したカード26を利用して自動的に入出金取引を

行う。また、これらの装置21、22は、通信回線27および通信制御装置23を介してホストコンピュータ24に接続される。さらに、ホストコンピュータ24にはデータベース25が接続される。

この端末装置21は、顧客が本人識別情報(暗証番号)を入力する際に用い、また、必要に応じてホストコンピュータ24からのメッセージを出力する。

また、カード読取装置22は、顧客により挿入されたカード26の内容を読み取ってホストコンピュータ24に渡す。

また、データベース25は、預金残高、取引種別等の情報や、暗証番号を定義する際に用いた個人的な嗜好情報(Individual Taste Information: ITI)を含む偽装情報(Camouflage Information: CI)の出力画面データを登録する。

また、ホストコンピュータ24は、暗証番号の確認処理を行う際のプログラムを格納する。

これにより、顧客が挿入したカード26から読

- 7 -

み取った情報に従って、データベース25に蓄積された出力画面データを端末装置21に表示し、その表示に従って顧客が端末装置21から選択・入力したデータと、予め設定した本人識別情報とを照合して、本人確認処理を行い、さらに自動取引を行う。

第3図は、本発明の第1の実施例における登録データ例図、第4図は本発明の第1の実施例におけるカード作成方法の説明図である。

本実施例では、顧客が自動取引を行う際に使用するカードの登録データは、個人的な嗜好情報(以下ITIと記す)等を基に作成する。つまり、第3者が推測し難い情報(本人の好きな色、身体特徴、趣味)を基に登録データを作成する。

さらに、カード作成時に、ITI情報とともに、偽装情報(以下CIと記す)も登録する。

例えば第3図のように、暗証番号の1桁目～4桁目のそれぞれに対応するITI情報およびCI情報を登録データとする。この場合、ITI情報は本人を識別するための真の情報であり、CI情

- 8 -

報は第3者による暗証番号の推測を防止するための偽装情報である。

また、第4図のように、カード41には暗証番号を直接登録せず、ITI情報番号およびシステム内に記憶したCI情報へのアクセスキーを登録する。これは、CI情報をカード内に登録すると、第3者によって解読される恐れがあるためである。なお、CI情報はシステム内に記憶する。

従って、カード41を作成する手順としては、銀行側(サービス提供者側)は予め全顧客に対応するITI情報とCI情報を作成し、CI情報へのアクセスキー番号を設定する。次に、顧客は自分のITI情報を決定する。次に、銀行側では顧客が指定したITI情報の値で自動取引用のカード41を作成して、顧客に提供する。これにより、顧客はITI情報を従来の暗証番号のように記憶する必要はない。すなわち、自動取引時の本人確認では、ITI情報およびCI情報を含む画面が表示されるため、本人の嗜好や特徴にあった項目を指示することにより暗証番号を入力できる。

第5図は、本発明の第1の実施例における自動取引システムの機能構成図である。

本実施例の自動取引システムは、カード読取部52、出力画面データファイル53、画面データ読込み処理部54、画面制御部55、入力データ処理部56、照合処理部57、およびカード返却部58を備える。

このカード読取部52は、顧客が挿入したカード51の内容を読み込み、画面データ読込み処理部54は、カード51内に登録されたCI情報へのアクセスキーをもとに、データベース25に格納された出力画面データファイル53から該当画面データを読み込む処理を行う。

また、画面制御部55は、顧客の入力に応じて表示する画面データを制御する。

また、入力データ処理部56は、表示画面の項目から顧客が選択した真の番号の入力データを処理する。なお、この入力データ(真の番号)は照合処理に使用される。

また、照合処理部57は、カード内に記憶され

たITI情報と、入力データ処理部56により入力された真の番号とを照合する。

また、カード返却部58は、処理終了後、顧客から挿入されたカード51を返却する。

第1図は、本発明の第1の実施例における自動取引システムの本人確認処理を示すフローチャート、第6図は本発明の第1の実施例における表示画面例図である。

このような構成により、本実施例の自動取引システムにおいて本人確認を行う場合には、第1図のように、顧客から挿入されたカードを読み込み(101)、そのカードに対応するCI情報へのアクセスキーおよびITI情報を記憶する(102)。

次に、ITIインデックスを1とし(103)、CI情報のアクセスキーによって、その顧客用の画面データを画面データファイル53から読み出す(104)。

その画面データを端末装置21にガイダンスとともに表示する(105)。例えば第6図①のように好きな色を問う画面が表示される。この場合、

- 11 -

顧客が選択すべき真の番号は3である。これにより、顧客は表示された項目の番号から真の番号を選択して入力する。

次に、顧客が入力した番号と、カード内のITI情報とが一致する場合には(106)、ITIインデックスの値を1アップし(107)、次の画面データを表示する。さらに、全ITI情報の照合が終了するまで(108)、暗証番号(4桁)の各桁に対応する画面が第6図②～④のように表示され、顧客の入力とカード内のITI情報との照合が行われる。

こうして全ての項目(4種類)について照合が完了し、登録した全てのITI情報が一致すると、顧客本人であることを確認し(109)、自動取引を行う(110)。

また、顧客が入力した番号と、カード内のITI情報とが一致しない場合には、照合エラー用の画面データを読み出して表示する(111)。

これらの処理が終了すると、顧客にカードを返却し(112)、処理を終了する。

- 13 -

- 12 -

なお、第1図におけるnはITI情報数であり、暗証番号が4桁の場合にはn=4である。

次に、本発明の第2の実施例について述べる。

本実施例の自動取引システムは、第1の実施例(第2図)と同様に、端末装置、カード読取装置、通信回線、ホストコンピュータ、およびデータベースを備え、顧客は本人確認情報を記憶したカードを利用して自動的に入出金取引を行う。

特に本実施例では、本人確認情報として定数を登録せず、照合コードを生成するためのアルゴリズムを登録し、さらに演算要素として定数および乱数を使用する。また、演算子として、+、-、×、÷、()、mod(a, b)等が使用できる。但し、÷は商の整数部、()は演算順序を規定するための括弧、mod(a, b)はbをaで割った剰余である。さらに、アクセスキーコードは、顧客の希望によって分割することが可能であり、各部分ごとにアルゴリズムを設定できる。また、演算結果が照合コードの桁数を超える場合は溢れた上位桁を捨て、また演算結果が負数の場合には絶対値を充てる。

- 14 -

また、データベースには、預金残高、取引種別等の情報や、本人確認情報を定義する際に用いるアクセスコード情報(ACI)を登録したアクセスコード情報ファイルを格納する。なお、アクセスコード情報としては、ID番号、照合コード(アクセスキーコード)を生成するためのアルゴリズム、キーコード構成、そのアルゴリズムの演算要素として用いる乱数の桁数等を登録する。

また、ホストコンピュータは、照合コードの確認処理を行う際のプログラムを格納する。

このような構成により、顧客が挿入したカードから読み取ったIDコードによりデータベースに蓄積されたアクセスコード情報を読み出し、乱数を発生して端末装置に表示し、その表示に従って顧客が端末装置から入力したコードと、予め登録したアルゴリズムにその乱数を代入して生成したコードとを照合して、本人確認処理を行い、さらに自動取引等のサービス提供を行う。

第7図は、本発明の第2の実施例における自動取引システムの機能構成図である。

第7図において、71はカード読取装置、72はカード読取部、73はアクセスコード情報(ACI)ファイル、74はディスプレイ制御部、75はアクセスコード情報読取部、76は乱数発生処理部、77はアクセスキーコード(AKC)作成処理部、78は入力コード照合処理部、79はキーボード読取部、80はサービス提供機能、81は端末装置のディスプレイ、82は端末装置のキーボード(KB)である。

このカード読取部72は、カード読取装置71が顧客のカードから読み取ったIDコードを受け取り、アクセスコード情報読取部75に渡す。

また、アクセスコード情報読取部75は、カードのIDコードにより、アクセス情報ファイル73から該当するアクセスコード情報を読み出し、乱数発生処理部76およびアクセスキーコード作成処理部77に渡す。

また、乱数発生処理部76は、アクセスコード情報読取部75から渡されたアクセスコード情報(乱数桁数)によって乱数を発生し、ディスプレイ

- 15 -

制御部74およびアクセスキーコード作成処理部77に渡す。

また、アクセスキーコード作成処理部77は、アクセスコード情報読取部75より得たアクセスコード情報(コード構成、生成アルゴリズム)と、乱数発生処理部76より得た乱数とから、照合コードを生成し、入力コード照合処理部78に渡す。

また、入力コード照合処理部78は、キーボード読取部79を介して顧客から得た入力コードと、アクセスキーコード作成処理部77より得た生成コードとを比較照合し、その結果がOKならば、サービス提供機能80へサービス許可の指示を出し、結果がNGならば、その通知をディスプレイ制御部74に渡す。

また、ディスプレイ制御部74は、端末装置のディスプレイ81を制御して、アクセスコード入力の案内、および乱数発生処理部76が発生した乱数を表示し、また、コード照合結果をメッセージとともに表示する。

次に、本実施例における本人確認処理を具体的

- 16 -

な例を挙げて述べる。

第8図は、本発明の第2の実施例におけるアクセスキーコードの構成例図、第9図は本発明の第2の実施例におけるアクセスコード情報例図、第10図は本発明の第2の実施例における自動取引システムの本人確認処理を示すフローチャートである。

本実施例では、契約時、顧客は“乱数の桁数”、“アクセスキーコードの構成”、および“照合コードを生成するためのアルゴリズム”を決定する。

例えば、乱数の桁数を4とし、アクセスキーコードの構成を第8図のように C_1 (2桁)、 C_2 、 C_3 の4桁として、アルゴリズムを“ $C_1 = 50 - RN_1$ 、 $C_2 = RN_1 + RN_2$ 、 $C_3 = RN_4 + 1$ ”とする。なお、 RN_1 、 RN_2 、 RN_4 はシステムが発生させる乱数の1、2、4桁目を示し、3桁目の乱数は表示されるのみで、照合コードの生成には用いられない。

また、システム側は、顧客の申告をID番号と対応させてアクセスコード情報ファイル73に記

憶する。

例えば、第9図のように、ID番号“123456”、乱数桁数“4”、キーコード要素数“3”、要素 C_1 の桁数“2”、要素 C_1 へのポインタ、要素 C_2 の桁数“1”、要素 C_2 へのポインタ、要素 C_3 の桁数“1”、要素 C_3 へのポインタ、およびアルゴリズム記述“ $C_1 = 50 - RN_1, C_2 = RN_1 + RN_2, C_3 = RN_4 + 1$ ”をアクセスコード情報ファイル73に記憶する。

こうして契約手続きが終了した後、顧客はカードを用いてサービスの提供を要求することができる。

すなわち、第10図のように、顧客がカードをカード読取装置71に挿入して読み取らせるか、あるいはID番号をキーボード82から入力すると(1001)、システム側では、そのID番号に対応するアクセスキーコード情報をアクセスコード情報ファイル73から読み出して(1002)、メモリに記憶する。

さらに、このアクセスキーコード情報により、

乱数桁数が4桁であることを知り、4桁の乱数を発生させて、メッセージとともにディスプレイ81に表示する(1003)。例えば、乱数を“ $RN_1 = 5, RN_2 = 9, RN_3 = 4, RN_4 = 1$ ”とする。

この表示により、顧客は予め登録したアルゴリズムを思い出し、表示された乱数をそれに代入してアクセスキーコードを作成し、キー入力する。

この場合、 $C_1 = 50 - RN_1 = 50 - 5 = 45$ 、 $C_2 = RN_1 + RN_2 = 5 + 9 = 14$ 、 $C_3 = RN_4 + 1 = 1 + 1 = 2$ となり、“4542”をキー入力する。なお、 C_2 は計算結果が予め決められた桁数を超えるため、下位の1桁を採る。また、表示された乱数の中、第3桁($RN_3 = 4$)は使用されないが、これは本人以外の利用者を惑わせるためである。

一方、システム側では、読み取ったアクセスキーコード情報から、アクセスキーコードを作成するアルゴリズム(要素数、各要素の桁数、各要素を算出する式)を知り、顧客に対して表示した乱数を当てはめて、“4542”を生成する(10

- 19 -

04)。

こうしてアクセスキーコードの入力が完了すると(1005)、顧客が入力したアクセスキーコードとシステム側で生成したコードとを比較照合する(1006)。

その結果、一致すれば(1007)、システムのサービス提供を許可し、一致しなければ(1007)、ディスプレイ81にエラーメッセージを出力する(1008)。

なお、本実施例では、4桁のアクセスキーコードを発生するアルゴリズムとして、乱数の第3桁を使用しない場合を示したが、この他にも種々の方法が考えられる。

例えば、乱数4桁で、アクセスキーコード構成を4要素各1桁(C_1, C_2, C_3, C_4)とし、アルゴリズムを $C_1 = 9, C_2 = RN_1, C_3 = RN_3, C_4 = RN_2$ とする。これにより、上位の1桁のみが固定的に“9”となり、その他は乱数によって変化するため、乱数“2068”を発生させた場合には、アクセスキーコードは“9860”とな

る。

また、例えば乱数9桁で、アクセスキーコード構成を3要素(C_1 は2桁、 C_2, C_3 は1桁)とし、アルゴリズムを $C_1 = 100 - RN_1 \times RN_1, C_2 = RN_1 + RN_2, C_3 = RN_9$ とする。これにより、9桁の乱数を発生しても、実際に用いるのは3桁であるため、容易に記憶でき、乱数“463831206”を発生させた場合には、アクセスキーコードは“8406”となる。

このように、提示する乱数は、1桁毎に分離して用いたり、全体を1個の数として使用したり、全く使用しない桁を設けたり、あるいは、同じ桁の数字を繰返して使用することができるため、多様なアルゴリズムを設定することが可能である。

また、パスワード中に本実施例の数列を組み込むことにより、コンピュータ端末からのアクセス時に、デタラメなコードを何度も試して正しいコードを探り当てる方法に対処することができる。

次に、本発明の第3の実施例について述べる。

本実施例の自動取引システムは、第1の実施例

(第2図)と同様に、端末装置、カード読取装置、通信回線、ホストコンピュータ、およびデータベースを備え、顧客は本人確認情報を記憶したカードを利用して自動的に入出金取引を行う。

また、本人確認情報として定数を登録せず、照合コードを生成するためのアルゴリズムを登録する。特に、演算要素として、年(Y)、月(M)、日(D)、時刻(H)、曜日(W)、定数、および顧客が代入する変数値(V_B (設定)、 V_R (参照))等であり、複数使用する場合は V_{B_i} のようにサフィックスを付ける)を使用する。さらに、演算子として、 $+$ 、 $-$ 、 \times 、 \div 、 $()$ 、 $\text{mod}(a, b)$ 等を使用する。

但し、 \div は商の整数部、 $()$ は演算順序を規定するための括弧、 $\text{mod}(a, b)$ は b を a で割った剰余である。さらに、年(Y)、月(M)、日(D)、時刻(H)および曜日(W)は、顧客がシステムにアクセスした時点の値を適用する。

また、 V_B は顧客が任意の数値を代入できる部分であり、その値はアクセスキーコードの別の部分を生成するために参照する。その参照値として

の表現形が V_R である。例えば、アクセスキーコードを2桁の数(C_1, C_2)とし、 $C_1 = V_B$ 、 $C_2 = 9 - V_R$ とした場合を述べる。顧客が第1桁に任意の数字“3”を入力し、 C_2 の V_R に“3”を代入すると、 $C_2 = 9 - 3 = 6$ となり、正しい入力コードは36である。このように、 V_B は $C_k = V_B$ の形で定義する。これらの演算要素により、より多様なアルゴリズムを設定できる。

また、データベースには、預金残高、取引種別等の情報や、本人確認情報を定義する際に用いるアクセスコード情報(ACI)を登録したアクセスコード情報ファイルを格納する。なお、アクセスコード情報としては、ID番号、照合コード(アクセスキーコード)を生成するためのアルゴリズム、キーコード構成を登録する。

また、ホストコンピュータは、照合コードの確認処理を行う際のプログラムを格納する。

第11図は、本発明の第3の実施例における自動取引システムの機能構成図である。

第11図において、71はカード読取装置、

- 23 -

72はカード読取部、73はアクセスコード情報(ACI)ファイル、74はディスプレイ制御部、75はアクセスコード情報読取部、77はアクセスキーコード(AKC)作成処理部、78は入力コード照合処理部、79はキーボード読取部、80はサービス提供機能、81は端末装置のディスプレイ、82は端末装置のキーボード(KB)である。

このカード読取部72は、カード読取装置71が顧客のカードから読み取ったIDコードを受け取り、アクセスコード情報読取部75に渡す。

また、アクセスコード情報読取部75は、カードのIDコードにより、アクセス情報ファイル73から該当するアクセスコード情報を読み出し、アクセスキーコード作成処理部77に渡す。

また、アクセスキーコード作成処理部77は、アクセスコード情報読取部75より得たアクセスコード情報(コード構成、生成アルゴリズム)から、生成コードを生成し、入力コード照合処理部78に渡す。また、入力コード照合処理部78は、キーボード読取部79を介して顧客から得た入力

- 24 -

コードと、アクセスキーコード作成処理部77より得た生成コードとを比較照合し、その結果をディスプレイ制御部74に渡す。

また、ディスプレイ制御部74は、端末装置のディスプレイ81を制御して、アクセスコード入力の案内、およびコード照合結果をメッセージとともに表示する。

次に、本実施例における本人確認処理を具体的な例を挙げて述べる。

第12図は、本発明の第3の実施例におけるアクセスコード情報例図、第13図は本発明の第3の実施例における自動取引システムのアクセス時の処理を示すフローチャートである。

本実施例では、顧客との契約時にアクセスコードの構成および算出アルゴリズムを決定する。

例えば、アクセスコードは4桁として、4個の構成要素に分割し、各構成要素は1桁とする。つまり、 C_1, C_2, C_3, C_4 を構成要素とする。また、算出アルゴリズムは、 $C_1 = V_B$ 、 $C_2 = 1$ 、 $C_3 = V_R + H$ 、 $C_4 = 5 + \text{mod}(3, D)$ とする。

この内容を、顧客のIDコードと対応させてアクセスコード情報ファイル73に登録する。すなわち、第12図のように、IDコード“123456”、キーコードの要素数“4”、要素1の桁数“1”、要素1へのポインタ、要素2の桁数“1”、要素2へのポインタ、要素3の桁数“1”、要素3へのポインタ、要素4の桁数“1”、要素4へのポインタ、およびアルゴリズム記述“ $C_1 = V_9$ 、 $C_2 = 1$ 、 $C_3 = V_R + H$ 、 $C_4 = 5 + \text{mod}(3, D)$ ”を登録する。

こうして契約を行い、システムへアクセスする場合には、第13図のように、顧客は磁気カードをカード読取部72に読み取らせるか、あるいはIDコードをキーボード82から入力する(1301)。

これにより、アクセス情報読取部75は、IDコードに対応するアクセスキーコード情報をアクセスコード情報ファイル73より読み出し、メモリへ記憶する(1302)。

次に、ディスプレイ制御部74の指示により、

アクセスコード入力促すメッセージをディスプレイに表示する(1303)。

この表示に従い、顧客は契約時に登録したアルゴリズムを想い出してキーコードを入力する。例えば、 $C_1 = V_9$ として任意の数字“7”をキーインし、 C_2 には固定の値“1”を入力する。また、 $C_3 = V_R + H$ には、 $V_9 = 7$ 、および現在の時刻“12時”から $H = 12$ を代入し、 $7 + 12 = 19$ を得るが、桁数が溢れているため、下1桁をとって $C_3 = V_R + H = 9$ を入力する。さらに、本日が“13日”であることから、 $C_4 = 5 + \text{mod}(3, D) = 5 + \text{mod}(3, 13) = 5 + 1 = 6$ を入力する。

こうしてアクセスコードが入力されると(1304)、アクセスキーコード作成処理部77は、アクセスコード情報からアクセスキーコード構成と生成アルゴリズムを知り、顧客が入力した V_9 、システムで管理している日付、時刻等を代入して、コードを生成する(1305)。

次に、入力コード照合処理部78は、アクセスキーコード作成処理部77で生成したコードと、

- 27 -

顧客が入力したアクセスキーコードとを比較照合し(1306)、一致すれば(1307)、サービス提供を許可する。また、一致しなければ、エラー処理を行う(1308)。

〔発明の効果〕

本発明によれば、自分の暗証番号を直接記憶する必要がないため、4桁前後の暗証番号に限定されることはなく、また、本人の嗜好や特徴等の情報を基にして定義するため、第三者が暗証番号を推測することは難しい。これにより、暗証番号の桁数を増加させることができる。

また、本発明によれば、アルゴリズムは無意味な数字よりも記憶し易く、逆に他人が推測することは難しい。さらに、そのアルゴリズムの演算要素としてシステムが発生させた乱数、あるいは年月日、時刻、曜日、任意の変数等を利用するため、アルゴリズムが推測できなければ、仮に、デタラメな入力でキーコードが偶然に一致することであっても、カードを連続して不正使用することはできない。

- 28 -

従って、システムのセキュリティをより高めることが可能である。

4. 図面の簡単な説明

第1図は本発明の第1の実施例における自動取引システムの本人確認処理を示すフローチャート、第2図は本発明の第1の実施例における自動取引システムの構成図、第3図は本発明の第1の実施例における登録データ例図、第4図は本発明の第1の実施例におけるカード作成方法の説明図、第5図は本発明の第1の実施例における自動取引システムの機能構成図、第6図は本発明の第1の実施例における表示画面例図、第7図は本発明の第2の実施例における自動取引システムの機能構成図、第8図は本発明の第2の実施例におけるアクセスキーコードの構成例図、第9図は本発明の第2の実施例におけるアクセスコード情報例図、第10図は本発明の第2の実施例における自動取引システムの本人確認処理を示すフローチャート、第11図は本発明の第3の実施例における自動取引システムの機能構成図、第12図は本発明の第

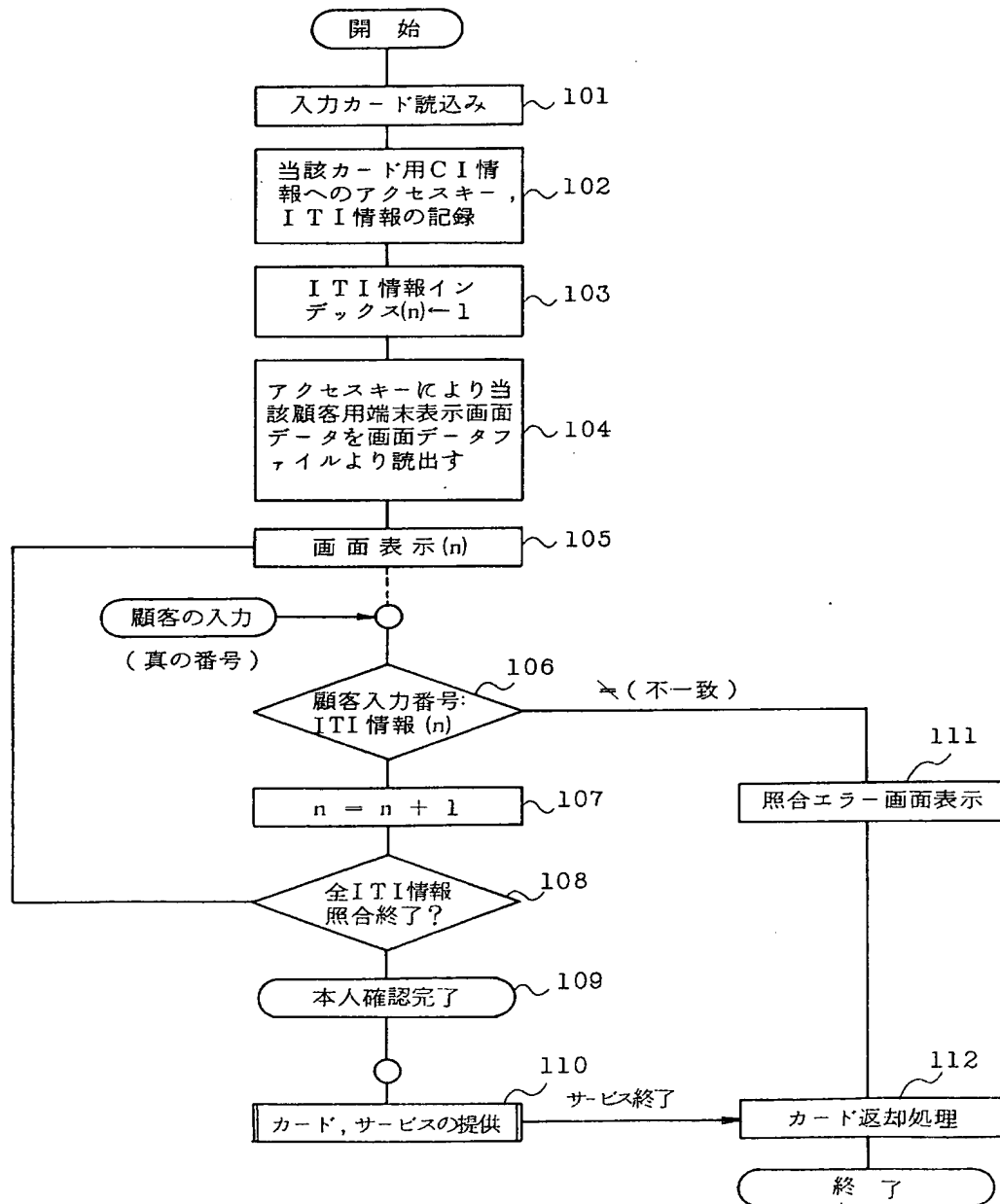
3の実施例におけるアクセスコード情報例図、第1.3図は本発明の第3の実施例における自動取引システムのアクセス時の処理を示すフローチャートである。

21: 端末装置, 22: カード読取装置, 23: 通信制御装置, 24: ホストコンピュータ, 25: データベース, 26, 41, 51: カード, 27: 通信回線, 52: カード読取部, 53: 出力画面データファイル, 54: 画面データ読込処理部, 55: 画面制御部, 56: 入力データ処理部, 57: 照合処理部, 58: カード返却部, 71: カード読取装置, 72: カード読取部, 73: アクセスコード情報(ACI)ファイル, 74: ディスプレイ制御部, 75: アクセスコード情報(ACI)読取部, 76: 乱数発生処理部, 77: アクセスキーワード(AKG)作成処理部, 78: 入力コード照合処理部, 79: キーボード読取部, 80: サービス提供機能, 81: 端末装置のディスプレイ, 82: 端末装置のキーボード(KB)。

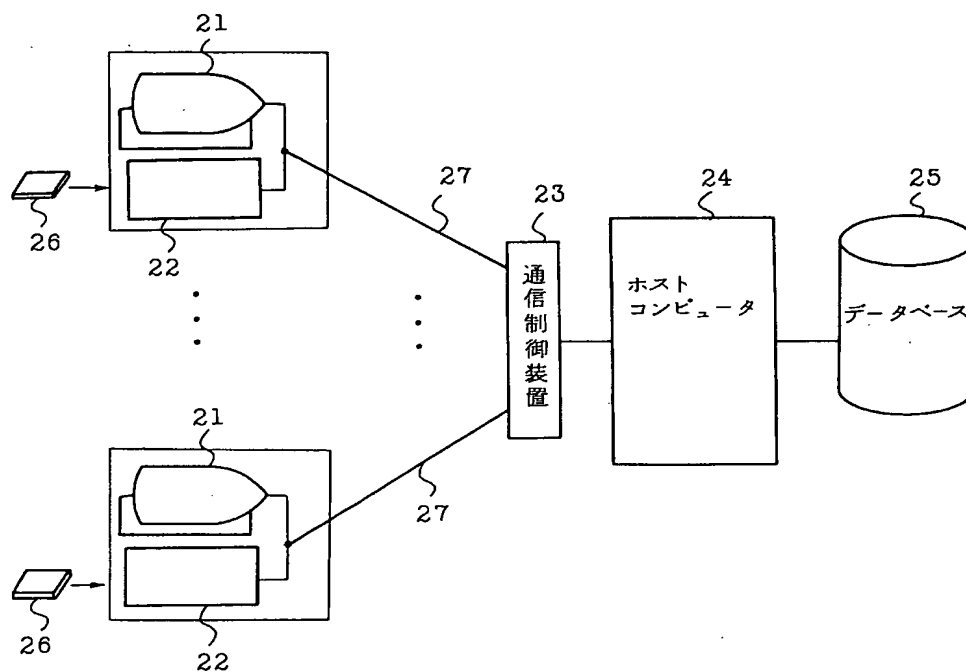
代 理 人 弁 理 士 磯 村 雅 俊



第 1 図



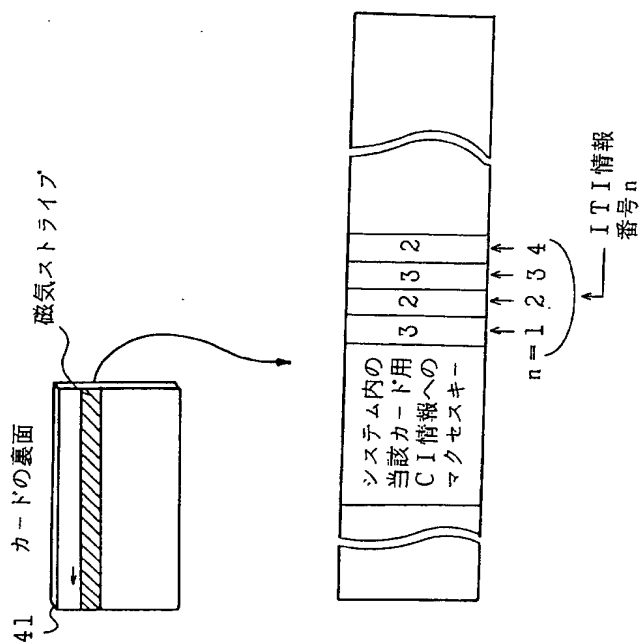
第 2 図



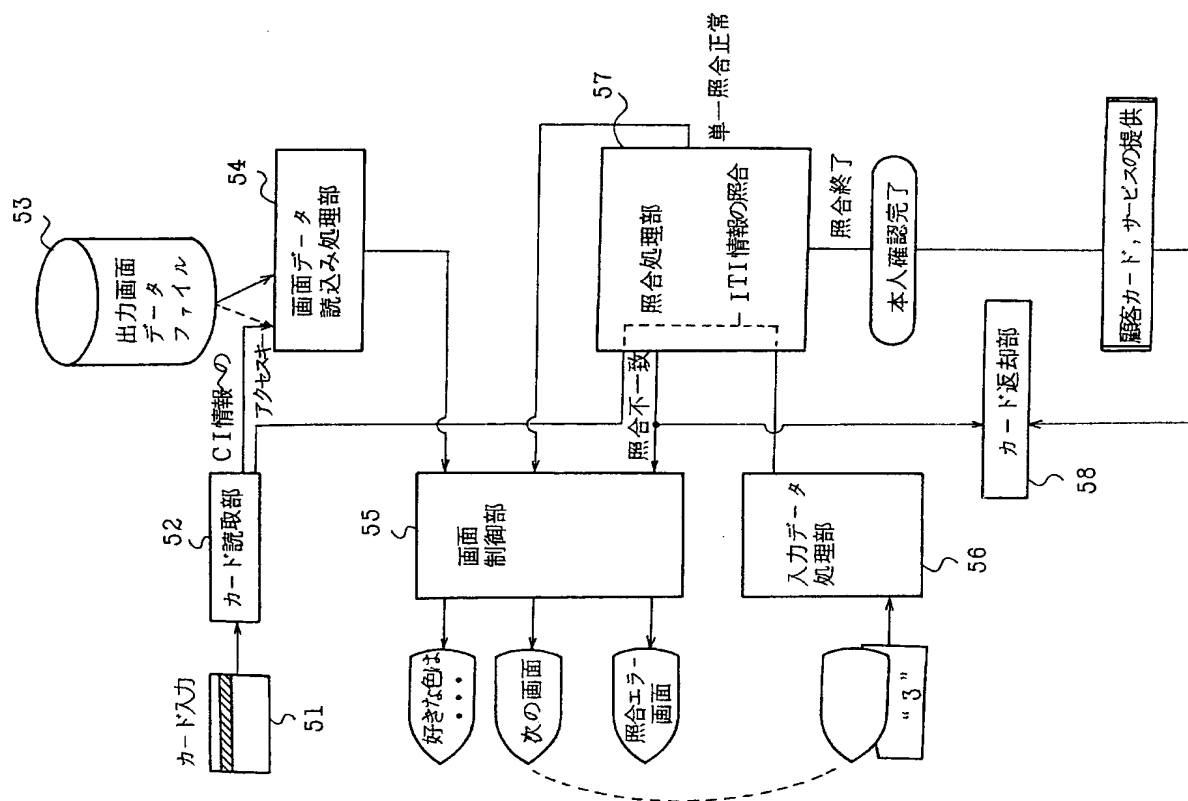
第 3 図

登録情報	I T I	C I
暗証番号の1桁目	好きな色は黄色	赤, 茶, 白, 黒...
" 2桁目	身長は175cm	180, 160, 165...
" 3桁目	家族は3人構成	4人, 2人, 1人...
" 4桁目	趣味はゴルフ	読書, 車...

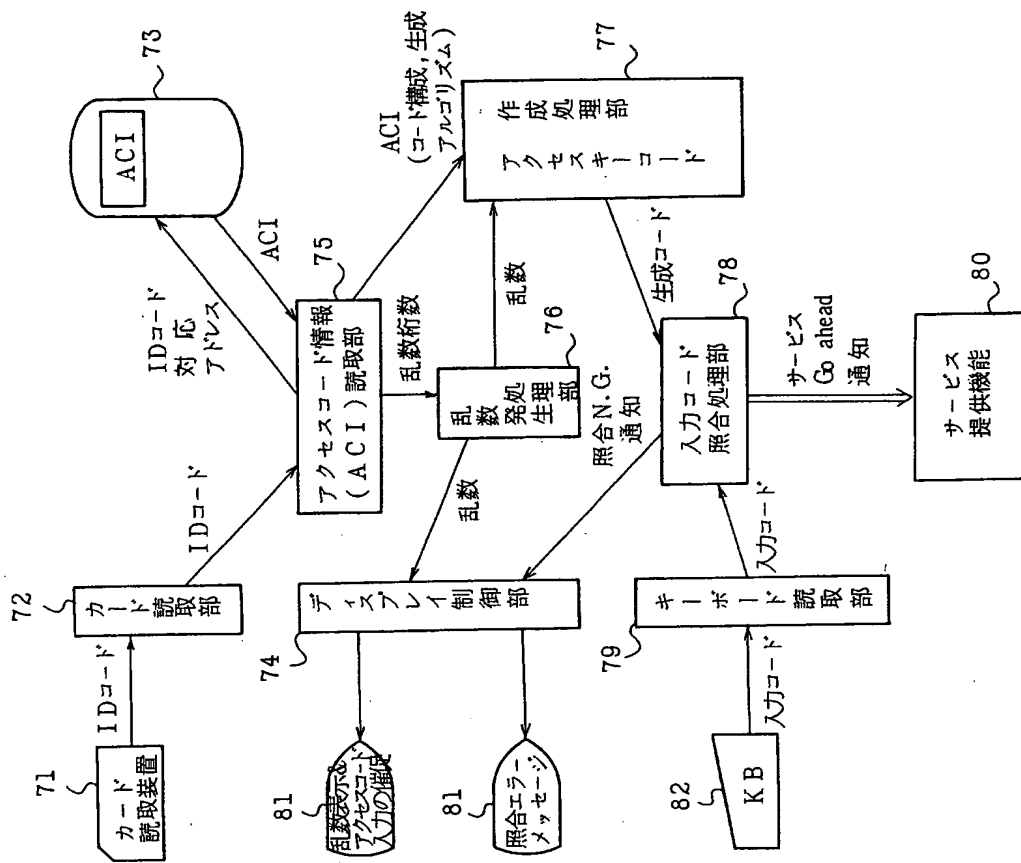
4 無



拆 5



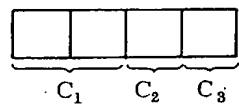
第 7 図



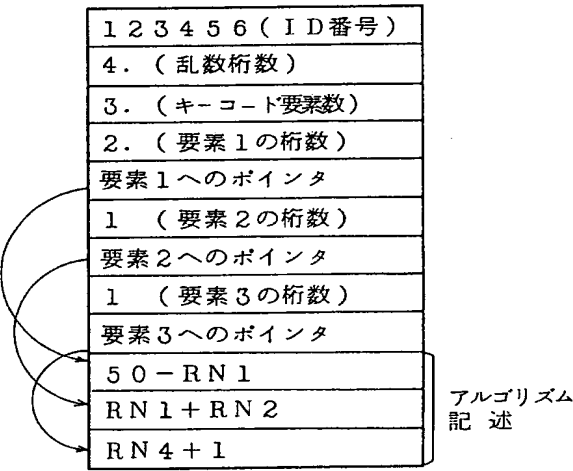
第 6 図

- ① 好きな色は何色ですか。
1 = 赤
2 = 茶
3 = 黄
4 = 白
5 = 黒
- ② 身長は何 cm ですか。
1 = 180 cm
2 = 175 cm
3 = 160 cm
4 = 165 cm
- ③ 家族は何人ですか。
1 = 4人
2 = 3人
3 = 2人
4 = 1人
- ④ 趣味は何ですか。
1 = 読書
2 = ゴルフ
3 = 車

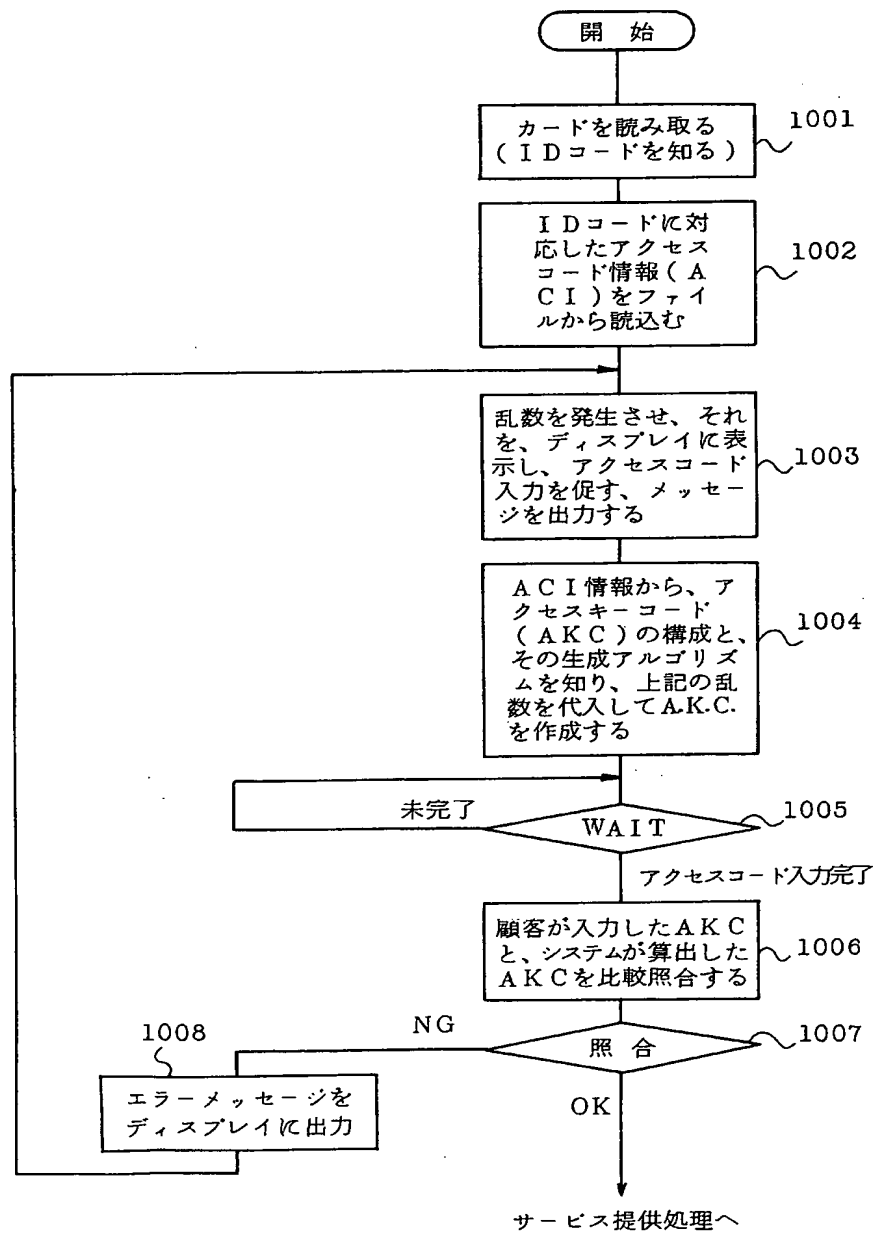
第 8 図



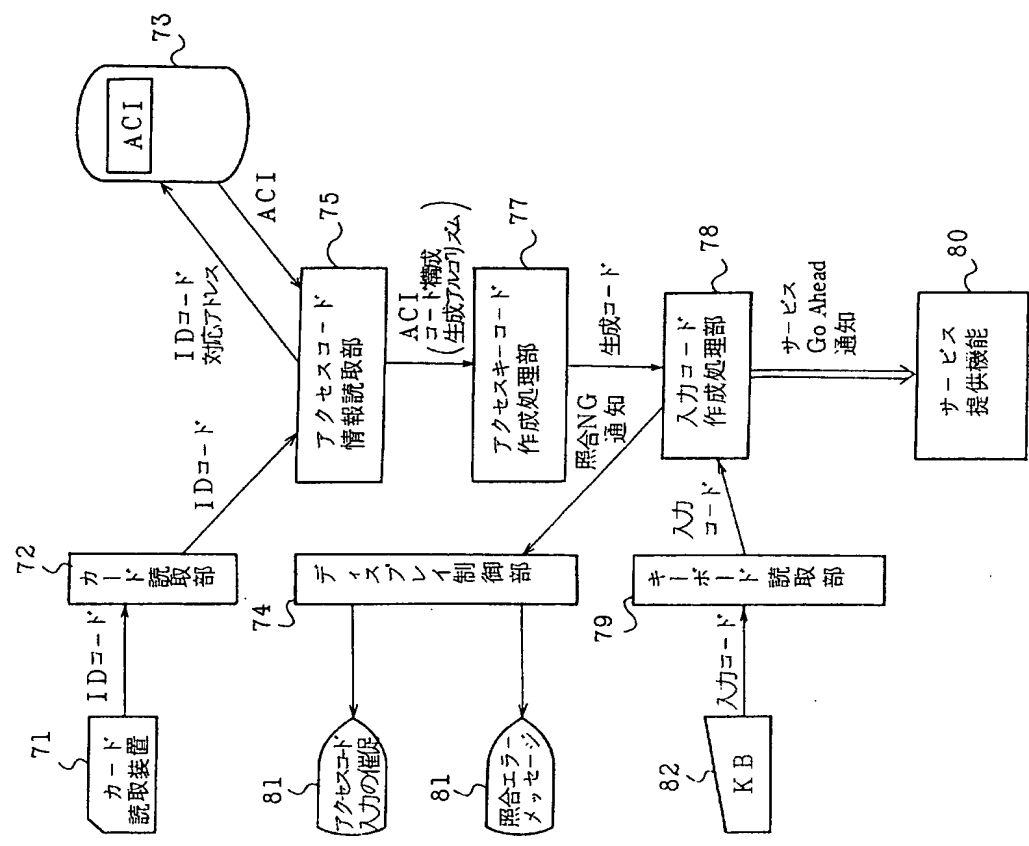
第 9 図



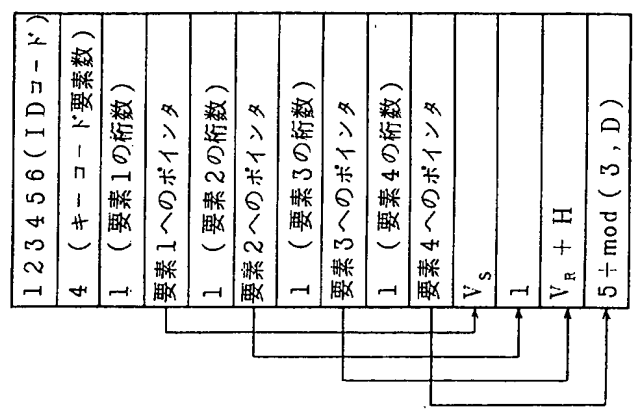
第 1 0 図



第 1 1 図



第 1 2 図



第 1 3 図

